

Technologie Sieciowe

Lista 1

Piotr Szymański

1. Opis programów

- 1.1. **Ping** - polecenie używane w sieciach komputerowych TCP/IP i służące do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie, czy istnieje połączenie pomiędzy hostami testującym i testowanym. Umożliwia on zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji, zwanych lagami.

1.1.1. Przykładowe użycie

```
C:\Users\piotr>ping facebook.com

Pinging facebook.com [185.60.216.35] with 32 bytes of data:
Reply from 185.60.216.35: bytes=32 time=26ms TTL=55
Reply from 185.60.216.35: bytes=32 time=26ms TTL=55
Reply from 185.60.216.35: bytes=32 time=26ms TTL=55
Reply from 185.60.216.35: bytes=32 time=53ms TTL=55

Ping statistics for 185.60.216.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 53ms, Average = 32ms
```

1.1.2. Najważniejsze opcje:

- t – pingowanie ustalonej witryny aż do przerwania instrukcji
- l - wartość – rozmiar wysłanego pakietu
- i – ustaw TTL(Time To Live)
- f – ustawienie flagi (DF) (Do not Fragment)

- 1.2. **Traceroute** – program służący do badania trasy pakietów sieci IP

1.2.1. Przykładowe użycie:

```
C:\Users\piotr>tracert facebook.com

Tracing route to facebook.com [185.60.216.35]
over a maximum of 30 hops:

  0  3 ms  2 ms  3 ms  lan.home [192.168.1.1]
  1  5 ms  4 ms  4 ms  wro-bng2.neo.tpnet.pl [83.1.5.3]
  2 10 ms  6 ms  4 ms  wro-r1.tpnet.pl [80.50.18.73]
  3  6 ms  6 ms  6 ms  poz-r1.tpnet.pl [194.204.175.205]
  4 30 ms 30 ms 29 ms ae104-10.ffttr6.-.opentransit.net [193.251.249.15]
  5 30 ms 30 ms 30 ms facebook-18.gw.opentransit.net [193.251.254.148]
  6 28 ms 26 ms 27 ms po141.asw01.fra2.tfbnw.net [204.15.21.250]
  7 26 ms 27 ms 27 ms po213.psw03.fra5.tfbnw.net [157.240.43.117]
  8 27 ms 27 ms 27 ms 173.252.67.135
  9 26 ms 26 ms 26 ms edge-star-mini-shv-01-frx5.facebook.com [185.60.216.35]

Trace complete.
```

- 1.3. **Wireshark** – sniffer będący wolnym oprogramowaniem. Umożliwia przechwytywanie i nagrywanie pakietów danych, a także ich dekodowanie. Dzięki dużej ilości dodatków potrafi rozpoznać i zdekodować wiele protokołów komunikacyjnych. W głównej mierze jest wykorzystywany przez administratorów sieci, służby specjalne oraz hakerów do śledzenia pakietów.

Przechwytywanie z Wi-Fi

Plik Edytuj Widok Idź Przechwyty Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc

Przebieg: filtr wybranej sieci: <Ctrl>/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|--------------------------------|-----------------|----------|--------|---|
| 560 | 44.914080 | 192.168.1.16 | 52.189.88.10 | TCP | 54 | 49769 → 443 [ACK] Seq=18517 Ack=8215 Win=66848 Len=0 |
| 561 | 45.996766 | 204.79.197.222 | 192.168.1.16 | TCP | 60 | 443 → 49731 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 562 | 46.128047 | 13.107.246.19 | 192.168.1.16 | TCP | 60 | 443 → 49730 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 563 | 47.509555 | 13.107.38.254 | 192.168.1.16 | TCP | 60 | 443 → 49730 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 564 | 49.598435 | 134.119.216.159 | 192.168.1.16 | TCP | 60 | [TCP Keep-Alive] 80 → 49684 [ACK] Seq=1 Ack=1 Win=254 Len=0 |
| 565 | 49.598480 | 192.168.1.16 | 134.119.216.159 | TCP | 54 | [TCP Keep-Alive ACK] 49684 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 |
| 566 | 50.817774 | 192.168.1.16 | 192.168.1.16 | ICMPv6 | 86 | Neighbor Solicitation for fe80::4a2c:a0ff:fe5b:96f7 from 3c17:18:65:e1:c8 |
| 567 | 51.095556 | fe80::3e17:18ff:fe6... ff02::1 | 192.168.1.255 | ICMPv6 | 86 | 57621 → 57621 Len=44 |
| 568 | 54.474910 | 192.168.1.21 | 192.168.1.255 | UDP | 86 | 57621 → 57621 Len=44 |
| 569 | 58.467879 | 192.168.1.16 | 104.26.11.240 | TCP | 54 | 49742 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0 |
| 570 | 58.468375 | 104.26.11.240 | 192.168.1.16 | TCP | 60 | 443 → 49742 [FIN, ACK] Seq=1 Ack=2 Win=57 Len=0 |
| 571 | 58.468388 | 192.168.1.16 | 104.26.11.240 | TCP | 54 | 49742 → 443 [ACK] Seq=2 Ack=2 Win=1024 Len=0 |
| 572 | 59.818112 | 134.119.216.159 | 192.168.1.16 | TCP | 60 | [TCP Keep-Alive] 80 → 49684 [ACK] Seq=1 Ack=1 Win=254 Len=0 |
| 573 | 59.818150 | 192.168.1.16 | 134.119.216.159 | TCP | 54 | [TCP Keep-Alive ACK] 49684 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 |
| 574 | 61.240219 | 89mcom-65-relic8 | Broadcast | ADP | 60 | Who has 192.168.1.1? Tell 192.168.1.1 |
| 575 | 61.561962 | 192.168.1.23 | 239.255.255.250 | SSDP | 216 | H-SEARCH * HTTP/1.1 |

1.4. Cloud computing

Model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez usługodawcę (wewnętrzny dział lub zewnętrzną organizację). Chmura to usługa oferowana przez dane oprogramowanie (oraz konieczną infrastrukturę). Oznacza to eliminację konieczności zakupu licencji czy konieczności instalowania i administracji oprogramowaniem. Konsument płaci za użytkowanie określonej usługi, np. za możliwość korzystania z arkusza kalkulacyjnego. Nie musi dokonywać zakupu sprzętu ani oprogramowania.

2. Testowanie:

2.1. Odległości:

Testy polegają na pingowaniu serwerów o różnej odległości geograficznej. Skoki do zostały ustalone poprzez znalezienie minimalnego ttl. Skoki z zostały ustalone poprzez różnicę między początkową wartością ttl (64, 128, 255), wartością otrzymaną w odpowiedzi pinga.

Wyniki zamieszczone zostały w tabeli poniżej.

| Adres | Położenie geograficzne | Skoki do | Skoki z | Średni czas |
|------------------|------------------------|----------|---------|-------------|
| facebook.com | California | 10 | 9 | 26ms |
| Kochamwroclaw.pl | Wrocław | 10 | 9 | 40ms |
| Taobao.com | Chiny | 41 | 36 | 312ms |
| Tourism.net.nz | Nowa Zelandia | 20 | 18 | 316ms |

2.2. Wielkość pakietów a ilość skoków

Sprawdzenie czy zmiana ilości wysyłanych pakietów zmienia liczbę skoków. Test przeprowadzany za pomocą flagi -l w instrukcji ping.

| Adres | 4 | 128 | 512 |
|----------------|----|-----|-----|
| Facebook.com | 10 | 10 | 10 |
| Taobao.com | 41 | 41 | 41 |
| Tourism.net.nz | 20 | 20 | 20 |

2.3. Wielkość pakietów a czas propagacji

Sprawdzamy czy większa ilość pakietów wpływa na czas propagacji. Test odbywa się za pomocą flagi -l w instrukcji ping.

Poniżej przedstawiono wyniki testów dla kolejno 4,128 oraz 1024 bajtów.

| Adres | 4 | 128 | 1024 |
|----------------|-----|-----|------|
| Facebook.com | 26 | 26 | 27 |
| Taobao.com | 304 | 306 | 307 |
| Tourism.net.nz | 321 | 321 | 307 |

2.4. Fragmentacja

Największy, możliwy do wysłania rozmiar niefragmentowanego pakietu jest równy 1472 bajty. Test został przeprowadzony za pomocą flag -l oraz -f instrukcji ping.

| Adres | Średni czas | Średni czas DF | TTL | TTL DF |
|----------------|-------------|----------------|-----|--------|
| Facebook.com | 26ms | 26ms | 55 | 55 |
| taobao.com | 392ms | 399ms | 88 | 88 |
| Tourism.net.nz | 317ms | 320ms | 46 | 46 |

3. Wnioski

Programy oferują szeroki zakres możliwości dotyczący zbierania informacji o sieci. Posiadają wiele ciekawych dodatkowych opcji, których znajomość znacznie rozszerza funkcjonalność programów.

Przeprowadzenie wielu testów bardzo pomogło w zrozumieniu działania sieci. Wyniki potwierdzają, że liczba skoków się powiększa w raz z odległością geograficzną, a liczba pakietów nie wpływa ani na trasę pakietu ani na czas propagacji. Również fragmentacja pakietów nie zmieniła czasu propagacji.